

kaspersky

Kaspersky Security Center

(version 13.0.0.11247)

Preparative Procedures

Document version: 2.01

10.09.2021

Table of contents

Table of contents	2
1. About this document	4
1.1. Terminology.....	4
1.2. References	4
1.3. Purpose of the document	4
2. Requirements and prerequisites	4
2.1. Required hardware and software	4
2.1.1. Administration Server.....	4
2.1.2. Web Console	7
2.1.3. Administration Console	9
2.1.4. Network Agent	9
2.2. Secure environment	12
2.2.1. Physical security	12
2.2.2. Trusted administration	12
2.2.3. Trusted platform.....	12
2.2.4. Time service.....	12
3. Pre-install procedures	12
3.1. OS setup.....	12
3.2. OS users password policy	12
3.3. Get and check an installation package.....	13
3.4. Install a database management system.....	13
4. Installation	13
4.1. Kaspersky Security Center installation.....	13
4.2. Web Console	22
4.2.1. Obtaining installation package	22
4.2.2. Web Console Setup installation	22
5. Post install setup	28
5.1. Quick Start Wizard.....	28
5.2. Setting up roles.....	29
5.3. Putting into evaluated configuration	29
5.3.1. Disabling mmc console ports (if MMC-based console is installed).....	29
5.3.2. Setting minimum TLS version	29
5.4. Setting the maximum number of events in the event repository	30
5.5. Rolling out to endpoint devices	30
5.5.1. Manual installation	30
5.5.2. Centralised rollout.....	31

5.5.3. Rollout by external means31

5.6. Checking KSC version installed32

1. About this document

1.1. Terminology

Terms and abbreviations used in this document are defined in [ST].

1.2. References

Reference	Document
[ST]	Kaspersky Security Center. Security Target. Version 2.01
[UGD]	Kaspersky Security Center. User Manual. Version 2.00

1.3. Purpose of the document

This document describes necessary preparative procedures for putting **Kaspersky Security Center (version 13.0.0.11247)** (hereinafter KSC) into the evaluated secure state as required by [ST]. [ST] contains certain assumptions and requirements for the operational environment that have to be fulfilled.

Users that aim to use the evaluated configuration of KSC in a secure way are required to follow the preparative procedures described in this document during installation and initial setup of KSC.

In order to fine-tune KSC settings according to organization needs and specific conditions, users should refer to [UGD] as guidance.

2. Requirements and prerequisites

2.1. Required hardware and software

This section lists hardware and software requirements consistent with the evaluated configuration. Users are encouraged to consult [UGD] sections “*Deployment best practices*” and “*Sizing Guide*” to determine hardware configuration that would be required for their enterprise size and layout, and logical structure of KSC installations.

2.1.1. Administration Server

Minimum hardware requirements:

- CPU with operating frequency of 1 GHz or higher. For a 64-bit operating system, the minimum CPU frequency is 1.4 GHz.
- RAM: 4 GB.
- Available disk space: 10 GB. When Vulnerability and Patch Management is used, at least 100 GB of free disk space must be available.

For deployment in cloud environments, the requirements for Administration Server and database server are the same as the requirements for physical Administration Server.

Software requirements:

- Microsoft® Data Access Components (MDAC) 2.8.
- Microsoft Windows® DAC 6.0.
- Microsoft Windows Installer 4.5.

- Operating system:
 - Microsoft Windows 10 20H2 32-bit/64-bit
 - Microsoft Windows 10 20H1 32-bit/64-bit
 - Microsoft Windows 10 Enterprise 2019 LTSC 32-bit/64-bit
 - Microsoft Windows 10 Enterprise 2016 LTSC 32-bit/64-bit
 - Microsoft Windows 10 Enterprise 2015 LTSC 32-bit/64-bit
 - Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809) 32-bit/64-bit
 - Microsoft Windows 10 Pro for Workstations RS5 (October 2018 Update, 1809) 32-bit/64-bit
 - Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809) 32-bit/64-bit
 - Microsoft Windows 10 Education RS5 (October 2018 Update, 1809) 32-bit/64-bit
 - Microsoft Windows 10 Pro 19H1 32-bit/64-bit
 - Microsoft Windows 10 Pro for Workstations 19H1 32-bit/64-bit
 - Microsoft Windows 10 Enterprise 19H1 32-bit/64-bit
 - Microsoft Windows 10 Education 19H1 32-bit/64-bit
 - Microsoft Windows 10 Home 19H2 32-bit/64-bit
 - Microsoft Windows 10 Pro 19H2 32-bit/64-bit
 - Microsoft Windows 10 Pro for Workstations 19H2 32-bit/64-bit
 - Microsoft Windows 10 Enterprise 19H2 32-bit/64-bit
 - Microsoft Windows 10 Education 19H2 32-bit/64-bit
 - Microsoft Windows 8.1 Pro 32-bit/64-bit
 - Microsoft Windows 8.1 Enterprise 32-bit/64-bit
 - Microsoft Windows 8 Pro 32-bit/64-bit
 - Microsoft Windows 8 Enterprise 32-bit/64-bit
 - Microsoft Windows 7 Professional with Service Pack 1 and higher 32-bit/64-bit
 - Microsoft Windows 7 Enterprise/Ultimate with Service Pack 1 and higher 32-bit/64-bit
 - Windows Server 2019 Standard 64-bit
 - Windows Server 2019 Core 64-bit
 - Windows Server 2019 Datacenter 64-bit
 - Windows Server 2016 Server Standard RS3 (v1709) (LTSC/CBB) 64-bit
 - Windows Server 2016 Server Datacenter RS3 (v1709) (LTSC/CBB) 64-bit
 - Windows Server 2016 Server Core RS3 (v1709) (Installation Option) (LTSC/CBB) 64-bit
 - Windows Server 2016 Standard (LTSC) 64-bit
 - Windows Server 2016 Server Core (Installation Option) (LTSC) 64-bit
 - Windows Server 2016 Datacenter (LTSC) 64-bit
 - Windows Server 2012 R2 Standard 64-bit
 - Windows Server 2012 R2 Server Core 64-bit
 - Windows Server 2012 R2 Foundation 64-bit
 - Windows Server 2012 R2 Essentials 64-bit

- Windows Server 2012 R2 Datacenter 64-bit
- Windows Server 2012 Standard 64-bit
- Windows Server 2012 Server Core 64-bit
- Windows Server 2012 Foundation 64-bit
- Windows Server 2012 Essentials 64-bit
- Windows Server 2012 Datacenter 64-bit
- Windows Server 2008 R2 Standard with Service Pack 1 and higher 64-bit
- Windows Server 2008 R2 with Service Pack 1 (all editions) 64-bit
- Windows Storage Server 2016 64-bit
- Windows Storage Server 2012 R2 64-bit
- Windows Storage Server 2012 64-bit
- Database server (can be installed on a different device):
 - Microsoft SQL Server 2012 Express 64-bit
 - Microsoft SQL Server 2014 Express 64-bit
 - Microsoft SQL Server 2016 Express 64-bit
 - Microsoft SQL Server 2017 Express 64-bit
 - Microsoft SQL Server 2019 Express 64-bit
 - Microsoft SQL Server 2014 (all editions) 64-bit
 - Microsoft SQL Server 2016 (all editions) 64-bit
 - Microsoft SQL Server 2017 (all editions) on Windows 64-bit
 - Microsoft SQL Server 2017 (all editions) on Linux 64-bit
 - Microsoft SQL Server 2019 (all editions) on Windows 64-bit (requires additional actions¹)
 - Microsoft SQL Server 2019 (all editions) on Linux 64-bit (requires additional actions²)
 - MySQL Standard Edition 5.7 32-bit/64-bit
 - MySQL Enterprise Edition 5.7 32-bit/64-bit
 - All supported SQL Server editions in Amazon RDS and Microsoft Azure cloud platforms
 - MariaDB Server 10.3 32-bit/64-bit with InnoDB storage engine³

The following virtual platforms are supported:

- VMware vSphere 6.7
- VMware vSphere 7.1
- VMware Workstation 15 Pro
- VMware Workstation 16 Pro
- Microsoft Hyper-V Server 2012 64-bit
- Microsoft Hyper-V Server 2012 R2 64-bit

¹ <https://help.kaspersky.com/KSC/13/en-US/92403.htm>

² <https://help.kaspersky.com/KSC/13/en-US/92403.htm>

³ It is recommended to use MariaDB 10.3.22; if use an earlier version, the Perform Windows update task might take more than one day to work.

- Microsoft Hyper-V Server 2016 64-bit
- Microsoft Hyper-V Server 2019 64-bit
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- Parallels Desktop 16
- Oracle VM VirtualBox 6.x (Windows guest login only)

The following SIEM systems are supported:

- HP (Micro focus) ArcSight ESM 7.0
- HP (Micro focus) ArcSight ESM 6.8
- IBM QRadar 7.4

2.1.2. Web Console

Kaspersky Security Center 13 Web Console (also referred to as Web Console) is an application that uses a web interface (Open API) provided by KSC for its management. Web Console was not evaluated as a part of KSC.

Minimum hardware requirements:

- CPU: 4 cores, operating frequency of 2.5 GHz
- RAM: 8 GB
- Available disk space: 40 GB

Software requirements:

- Operating system Microsoft Windows (64-bit versions only), one of the following:
 - Microsoft Windows 10 20H2
 - Microsoft Windows 10 20H1
 - Microsoft Windows 10 Enterprise 2019 LTSC
 - Microsoft Windows 10 Enterprise 2016 LTSC
 - Microsoft Windows 10 Enterprise 2015 LTSC
 - Microsoft Windows 10 Pro RS5 (October 2018 Update, 1809)
 - Microsoft Windows 10 Pro for Workstations RS5 (October 2018 Update, 1809)
 - Microsoft Windows 10 Enterprise RS5 (October 2018 Update, 1809)
 - Microsoft Windows 10 Education RS5 (October 2018 Update, 1809)
 - Microsoft Windows 10 Pro 19H1
 - Microsoft Windows 10 Pro for Workstations 19H1
 - Microsoft Windows 10 Enterprise 19H1
 - Microsoft Windows 10 Education 19H1
 - Microsoft Windows 10 Home 19H2
 - Microsoft Windows 10 Pro 19H2
 - Microsoft Windows 10 Pro for Workstations 19H2
 - Microsoft Windows 10 Enterprise 19H2
 - Microsoft Windows 10 Education 19H2
 - Microsoft Windows 8.1 Pro
 - Microsoft Windows 8.1 Enterprise
 - Windows Server 2019 Standard
 - Windows Server 2019 Core
 - Windows Server 2019 Datacenter

- Windows Server 2016 Server Standard RS3 (v1709) (LTSB/CBB)
- Windows Server 2016 Server Datacenter RS3 (v1709) (LTSB/CBB)
- Windows Server 2016 Server Core RS3 (v1709) (Installation Option) (LTSB/CBB)
- Windows Server 2016 Standard (LTSB)
- Windows Server 2016 Server Core (Installation Option) (LTSB)
- Windows Server 2016 Datacenter (LTSB)
- Windows Server 2012 R2 Standard
- Windows Server 2012 R2 Server Core
- Windows Server 2012 R2 Foundation
- Windows Server 2012 R2 Essentials
- Windows Server 2012 R2 Datacenter
- Windows Server 2012 Standard
- Windows Server 2012 Server Core
- Windows Server 2012 Foundation
- Windows Server 2012 Essentials
- Windows Server 2012 Datacenter
- Windows Storage Server 2016
- Windows Storage Server 2012 R2
- Windows Storage Server 2012
- Linux (64-bit versions only):
 - Debian GNU/Linux 10.x (Buster)
 - Debian GNU/Linux 9.x (Stretch)
 - Ubuntu Server 20.04 LTS (Focal Fossa)
 - Ubuntu Server 18.04 LTS (Bionic Beaver)
 - CentOS 8.x
 - CentOS 7.x
 - Red Hat Enterprise Linux Server 8.x
 - Red Hat Enterprise Linux Server 7.x
 - SUSE Linux Enterprise Server 15 (all Service Packs)
 - SUSE Linux Enterprise Server 12 (all Service Packs)
 - Astra Linux Special, version 1.6
 - Astra Linux Special, version 1.5
 - Astra Linux Common Edition, version 2.12
 - ALT 9.1
 - ALT 8.3
 - ALT SE 8
- Node.js 14.16.1

Browser:

For a client, use of Kaspersky Security Center 13 Web Console only requires a browser, one of the following:

- Mozilla Firefox 68 Extended Support Release
- Mozilla Firefox 68 or later
- Google Chrome 75 or later
- Safari 12 on macOS
- Safari 13 on iOS

The hardware and software requirements for the device are identical to the requirements of the chosen browser that is used with Kaspersky Security Center 13 Web Console.

2.1.3. Administration Console

Minimum hardware requirements:

- CPU: with operating frequency of 1 GHz or higher. For a 64-bit OS, the minimum CPU frequency is 1.4 GHz.
- RAM: 512 MB.
- Available disk space: 1 GB.

Software requirements:

- Microsoft Windows operating system (supported version of the operating system is determined by the requirements of Administration Server), **except** for the following operating systems:
 - Windows Server 2012 Server Core 64-bit
 - Windows Server 2012 R2 Server Core 64-bit
 - Windows Server 2016 Server Core (Installation Option) (LTSB) 64-bit
 - Windows Server 2016 Server Datacenter RS3 (v1709) (LTSB/CBB) 64-bit
 - Windows Server 2016 Server Standard RS3 (v1709) (LTSB/CBB) 64-bit
 - Windows Server 2016 Server Core RS3 (v1709) (Installation Option) (LTSB/CBB) 64-bit
 - Windows Server 2019 Core 64-bit
- Microsoft Management Console 2.0
- Microsoft Windows Installer 4.5
- Microsoft Internet Explorer 10.0 running on:
 - Microsoft Windows Server 2008 R2 Service Pack 1
 - Microsoft Windows Server 2012
 - Microsoft Windows Server 2012 R2
 - Microsoft Windows 7 Service Pack 1
 - Microsoft Windows 8
 - Microsoft Windows 8.1
 - Microsoft Windows 10
- Microsoft Internet Explorer 11.0 running on:
 - Microsoft Windows Server 2012 R2
 - Microsoft Windows Server 2012 R2 Service Pack 1
 - Microsoft Windows Server 2016
 - Microsoft Windows Server 2019
 - Microsoft Windows 7 Service Pack 1
 - Microsoft Windows 8.1
 - Microsoft Windows 10
- Microsoft Edge running on Microsoft Windows 10

2.1.4. Network Agent

Minimum hardware requirements:

- CPU with operating frequency of 1 GHz or higher. For a 64-bit OS, the minimum CPU frequency is 1.4 GHz.
- RAM: 512 MB.
- Available disk space: 1 GB.

Software requirements:

- Operating system, one of the following:

- Microsoft Windows Embedded POSReady 2009 with latest Service Pack 32-bit
- Microsoft Windows Embedded POSReady 7 32-bit/64-bit
- Microsoft Windows Embedded Standard 7 with Service Pack 1 32-bit/64-bit
- Microsoft Windows Embedded 8 Standard 32-bit/64-bit
- Microsoft Windows Embedded 8.1 Industry Pro 32-bit/64-bit
- Microsoft Windows Embedded 8.1 Industry Enterprise 32-bit/64-bit
- Microsoft Windows Embedded 8.1 Industry Update 32-bit/64-bit
- Microsoft Windows 10 20H2 32-bit/64-bit
- Microsoft Windows 10 20H1 32-bit/64-bit
- Microsoft Windows 10 Enterprise 2015 LTSB 32-bit/64-bit
- Microsoft Windows 10 Enterprise 2016 LTSB 32-bit/64-bit
- Microsoft Windows 10 Enterprise 2019 LTSC 32-bit/64-bit
- Microsoft Windows 10 Home RS5 (Oct 2018) 32-bit/64-bit
- Microsoft Windows 10 Pro RS5 (Oct 2018) 32-bit/64-bit
- Microsoft Windows 10 Pro for Workstations RS5 (Oct 2018) 32-bit/64-bit
- Microsoft Windows 10 Enterprise RS5 (Oct 2018) 32-bit/64-bit
- Microsoft Windows 10 Education RS5 (Oct 2018) 32-bit/64-bit
- Microsoft Windows 10 Home RS4 (April 2018 Update, 17134) 32-bit/64-bit
- Microsoft Windows 10 Pro RS4 (April 2018 Update, 17134) 32-bit/64-bit
- Microsoft Windows 10 Pro for Workstations RS4 (April 2018 Update, 17134) 32-bit/64-bit
- Microsoft Windows 10 Enterprise RS4 (April 2018 Update, 17134) 32-bit/64-bit
- Microsoft Windows 10 Education RS4 (April 2018 Update, 17134) 32-bit/64-bit
- Microsoft Windows 10 Home RS3 (Fall Creators Update, v1709) 32-bit/64-bit
- Microsoft Windows 10 Pro RS3 (Fall Creators Update, v1709) 32-bit/64-bit
- Microsoft Windows 10 Pro for Workstations RS3 (Fall Creators Update, v1709) 32-bit/64-bit
- Microsoft Windows 10 Enterprise RS3 (Fall Creators Update, v1709) 32-bit/64-bit
- Microsoft Windows 10 Education RS3 (Fall Creators Update, v1709) 32-bit/64-bit
- Microsoft Windows 10 Home 19H1 32-bit/64-bit
- Microsoft Windows 10 Pro 19H1 32-bit/64-bit
- Microsoft Windows 10 Pro for Workstations 19H1 32-bit/64-bit
- Microsoft Windows 10 Enterprise 19H1 32-bit/64-bit
- Microsoft Windows 10 Education 19H1 32-bit/64-bit
- Microsoft Windows 10 Home 19H2 32-bit/64-bit
- Microsoft Windows 10 Pro 19H2 32-bit/64-bit
- Microsoft Windows 10 Pro for Workstations 19H2 32-bit/64-bit
- Microsoft Windows 10 Enterprise 19H2 32-bit/64-bit
- Microsoft Windows 10 Education 19H2 32-bit/64-bit
- Microsoft Windows 8.1 Pro 32-bit/64-bit
- Microsoft Windows 8.1 Enterprise 32-bit/64-bit
- Microsoft Windows 8 Pro 32-bit/64-bit
- Microsoft Windows 8 Enterprise 32-bit/64-bit
- Microsoft Windows 7 Professional with Service Pack 1 and higher 32-bit/64-bit
- Microsoft Windows 7 Enterprise/Ultimate with Service Pack 1 and higher 32-bit/64-bit
- Microsoft Windows 7 Home Basic/Premium with Service Pack 1 and higher 32-bit/64-bit
- Microsoft Windows XP Professional for Embedded Systems 32-bit
- Microsoft Windows XP Professional Service Pack 3 and higher 32-bit
- Windows Small Business Server 2011 Essentials 64-bit
- Windows Small Business Server 2011 Premium Add-on 64-bit
- Windows Small Business Server 2011 Standard 64-bit
- Windows MultiPoint Server 2011 Standard/Premium 64-bit
- Windows MultiPoint Server 2012 Standard/Premium 64-bit
- Windows Server 2008 R2 Standard Service Pack 1 and higher 64-bit
- Windows Server 2008 R2 Datacenter Service Pack 1 and higher 64-bit

- Windows Server 2008 R2 Enterprise Service Pack 1 and higher 64-bit
 - Windows Server 2008 R2 Foundation with Service Pack 1 and higher 64-bit
 - Windows Server 2008 R2 Service Pack 1 and higher Core Mode 64-bit
 - Windows Server 2008 R2 Service Pack 1 (all editions) 64-bit
 - Windows Server 2012 Server Core 64-bit
 - Windows Server 2012 Datacenter 64-bit
 - Windows Server 2012 Essentials 64-bit
 - Windows Server 2012 Foundation 64-bit
 - Windows Server 2012 Standard 64-bit
 - Windows Server 2012 R2 Server Core 64-bit
 - Windows Server 2012 R2 Datacenter 64-bit
 - Windows Server 2012 R2 Essentials 64-bit
 - Windows Server 2012 R2 Foundation 64-bit
 - Windows Server 2012 R2 Standard 64-bit
 - Windows Server 2016 Datacenter (LTSB) 64-bit
 - Windows Server 2016 Standard (LTSB) 64-bit
 - Windows Server 2016 Server Core (Installation Option) (LTSB) 64-bit
 - Windows Server 2016 Server Datacenter RS3 (v1709) (LTSB/CBB) 64-bit
 - Windows Server 2016 Server Standard RS3 (v1709) (LTSB/CBB) 64-bit
 - Windows Server 2016 Server Core RS3 (v1709) (Installation Option) (LTSB/CBB) 64-bit
 - Windows Server 2019 Standard 64-bit
 - Windows Server 2019 Core 64-bit
 - Windows Server 2019 Datacenter 64-bit
 - Windows Storage Server 2016 64-bit
 - Windows Storage Server 2012 64-bit
 - Windows Storage Server 2012 R2 64-bit
 - Debian GNU/Linux 10.x (Buster) 32-bit/64-bit
 - Debian GNU/Linux 9.x (Stretch) 32-bit/64-bit
 - Ubuntu Server 20.04 LTS (Focal Fossa) 32-bit/64-bit
 - Ubuntu Server 18.04 LTS (Bionic Beaver) 32-bit/64-bit
 - Ubuntu Desktop 20.04 LTS (Focal Fossa) 32-bit/64-bit
 - Ubuntu Desktop 18.04 LTS (Bionic Beaver) 32-bit/64-bit
 - CentOS 8.x 64-bit
 - CentOS 7.x 64-bit
 - Red Hat Enterprise Linux Server 8.x 64-bit
 - Red Hat Enterprise Linux Server 7.x 64-bit
 - SUSE Linux Enterprise Server 15 (all Service Packs) 64-bit
 - SUSE Linux Enterprise Desktop 15 (all Service Packs) 64-bit
 - SUSE Linux Enterprise Server 12 (all Service Packs) 64-bit
 - Astra Linux Special, version 1.6
 - Astra Linux Special, version 1.5
 - Astra Linux Common Edition, version 2.12
 - ALT 9.1
 - ALT 8.3
 - ALT SE 8
 - OS X 10.10 (Yosemite)
 - OS X 10.11 (El Capitan)
 - macOS Sierra (10.12)
 - macOS High Sierra (10.13)
 - macOS Mojave (10.14)
 - macOS Catalina (10.15)
 - macOS Big Sur (11.x)
- The following virtualization platforms are supported:

- VMware Workstation 16 Pro
- VMware Workstation 15 Pro
- Microsoft Hyper-V Server 2012 64-bit
- Microsoft Hyper-V Server 2012 R2 64-bit
- Microsoft Hyper-V Server 2016 64-bit
- Microsoft Hyper-V Server 2019 64-bit
- Citrix XenServer 7.1 LTSR
- Citrix XenServer 8.x
- VMware vSphere 7.1
- VMware vSphere 6.7

2.2. Secure environment

The following requirements have to be met for secure operation of KSC. When deploying and using KSC, its users should make sure those requirements are met.

2.2.1. Physical security

KSC and RDBMS should be installed on the hardware that will prevent unauthorised physical access to their components and parts.

2.2.2. Trusted administration

The personnel responsible for KSC administration and administration of underlying system and RDBMS should be trustworthy. They should follow this document and [UGD] while managing and using the system and perform all tasks correctly and with regards to the KSC security.

2.2.3. Trusted platform

The KSC server device shall be located in a trusted environment that provides strong physical and logical access restrictions. Platform should be set up in a secure way to minimise risk of unauthorised access to KSC or RDBMS data.

Underlying platform and operating system should be trusted to correctly perform their functions.

2.2.4. Time service

The platform should be configured to provide KSC with accurate and reliable timestamps.

3. Pre-install procedures

3.1. OS setup

An operating system and all prerequisites must be installed on a target device. Also make sure your device has no Network Agent installed.

3.2. OS users password policy

Operating system administrators and users that are supposed to have access to the TOE functionality are obliged to follow the certain password policy:

- a) Characters allowed:

- A – Z
 - a – z
 - 0 – 9
 - @ # \$ % ^ & * - _ ! + = [] { } | \ : ' , . ? / ` ~ " () ;
- b) Characters disallowed:
- Unicode characters
 - spaces
 - Cannot contain a dot character '.' immediately preceding the '@' symbol
- c) Password restrictions:
- 8 characters minimum and 16 characters maximum
 - Must contain characters at least from any 3 of 4 groups mentioned in the section "Characters allowed".

3.3. Get and check an installation package

Download an installation package from Kaspersky Lab support website <https://support.kaspersky.com/15020>.

Compare checksums of the TOE with ones listed in [ST] to make sure you are using the certified package.

You may use tools of your choice that support calculation of SHA256 hash or CertUtil tool included into MS Windows installation. In latter case you should use following command:

```
c:\>certutil -hashfile <path-to-file> sha256
```

Compare the calculated checksum to the one listed in [ST] and/or published on the Kaspersky Lab website.

3.4. Install a database management system

Before the Kaspersky Security Center installation, you must install a database management system (RDBMS) that will be used by Kaspersky Security Center. You can choose one from the supported versions of Microsoft SQL Server or MySQL.

For information about how to install the selected RDBMS, please refer to its documentation.

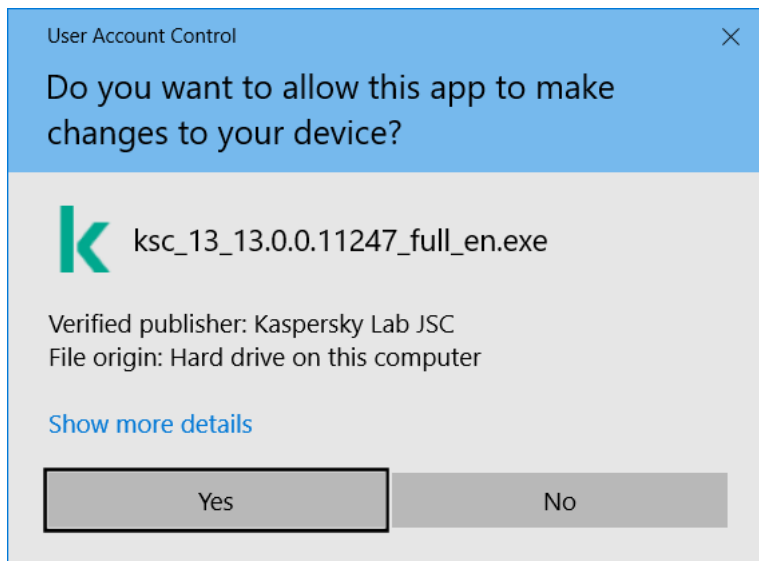
4. Installation

4.1. Kaspersky Security Center installation

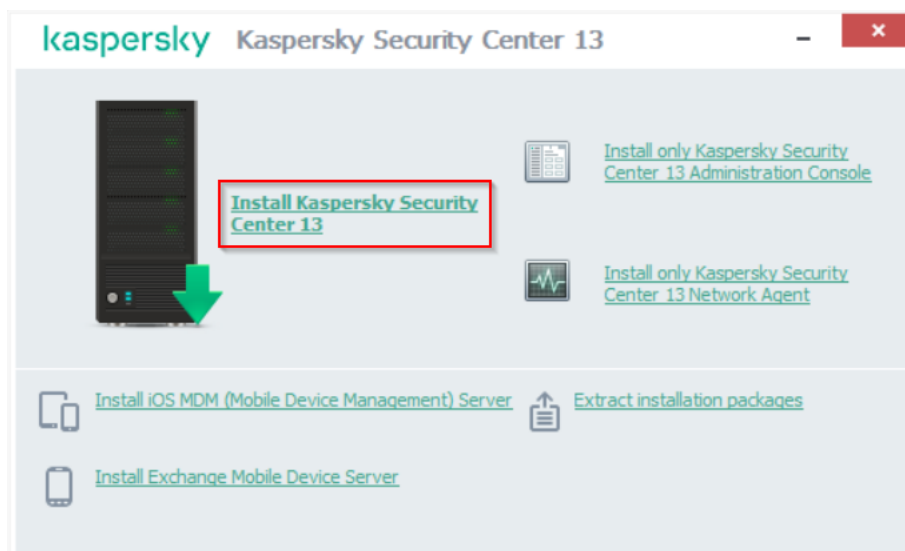
This procedure describes how to install Kaspersky Security Center.

1. Under an account with administrative privileges, run the `ksc_13_13.0.0.11247_full_en.exe` executable file.

2. Allow the app to make changes to your device, if asked.

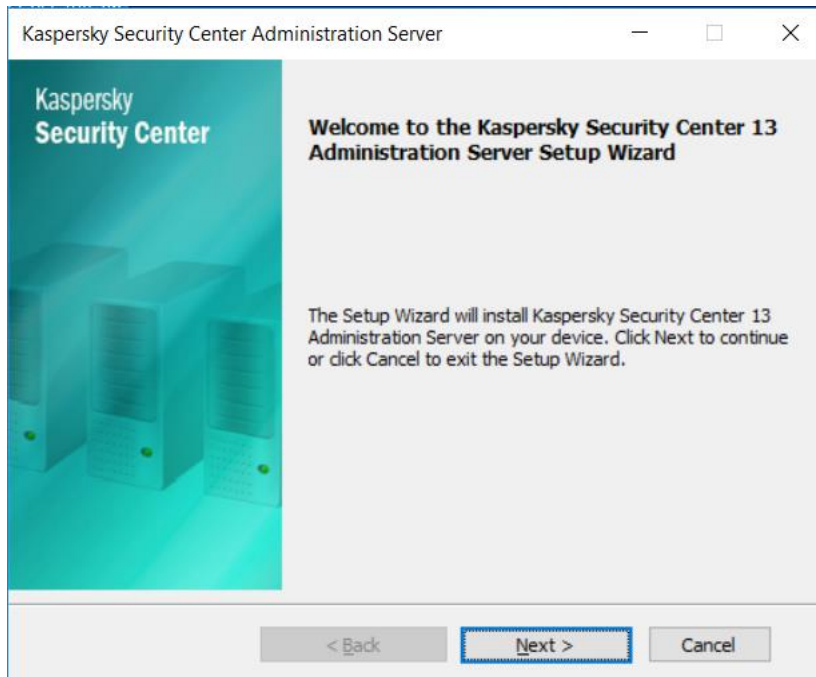


3. In the application selection window that opens, click **Install Kaspersky Security Center 13**.

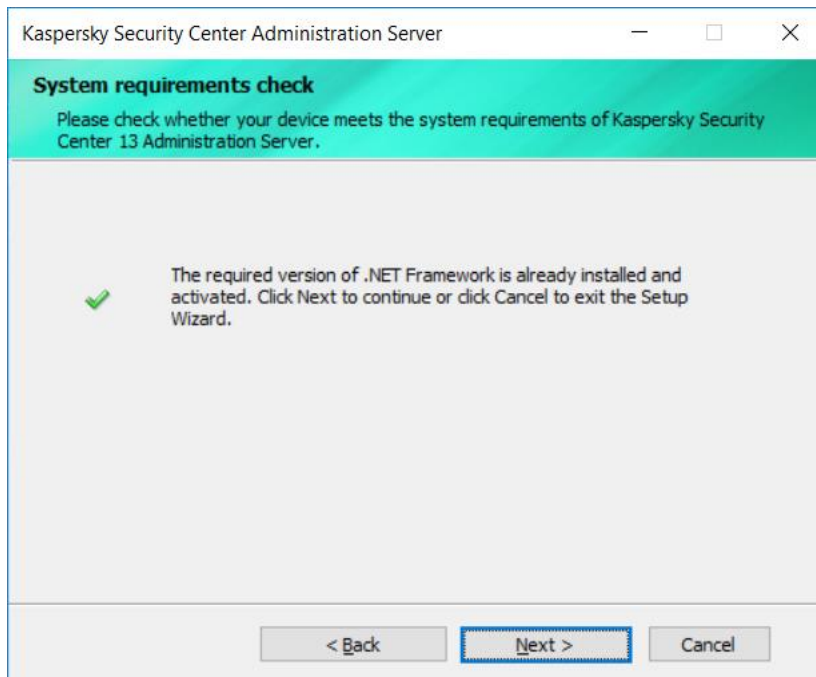


4. Please wait until the app is extracted and prepared for installation. Then the Setup Wizard of Kaspersky Security Center 13 Administration Server starts. Beginning with the Welcome page, proceed through the

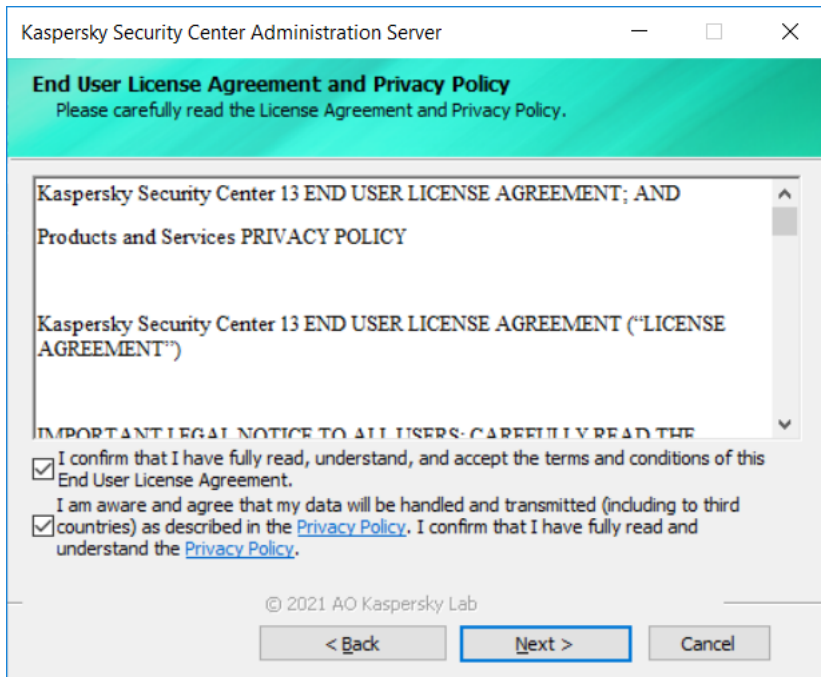
Wizard by clicking the **Next** button.



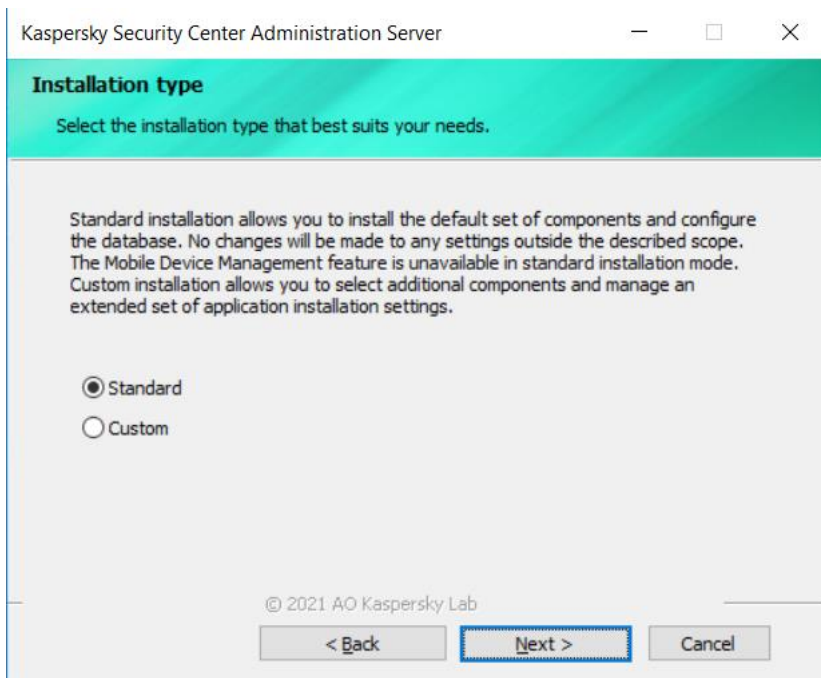
5. If Microsoft .NET Framework is not installed, install it. Otherwise click **Next**.



6. Read and accept the terms and conditions of the End User License Agreement and Privacy Policy.

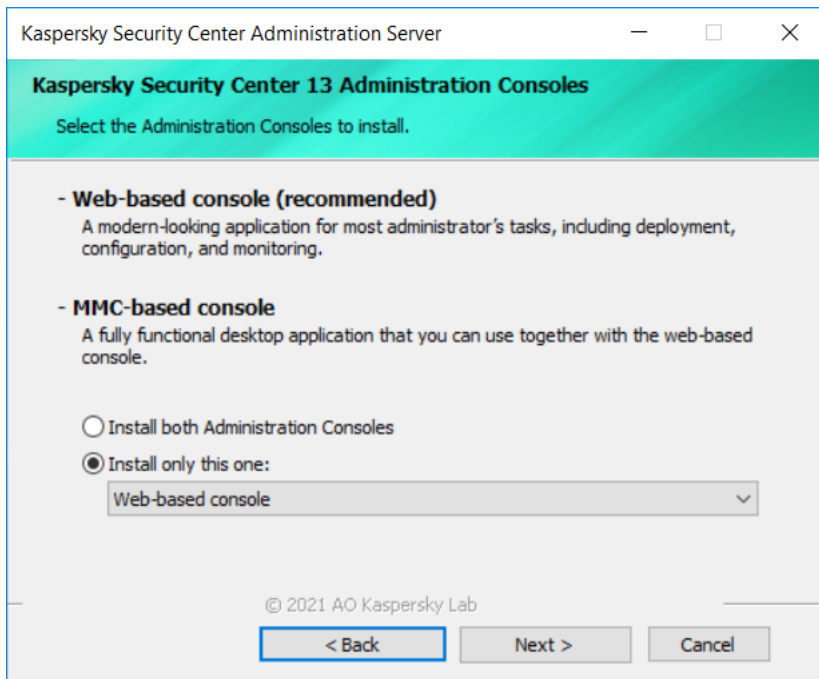


7. Select the installation type. For the evaluated configuration keep the default **Standard** value.

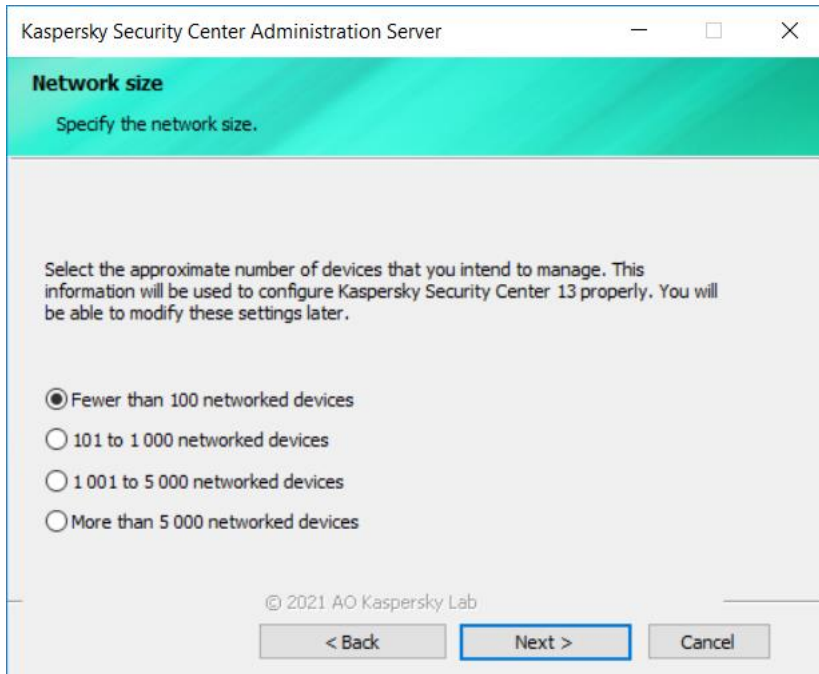


8. If you want to install Kaspersky Security Center 13 Web Console on the same device with Administration Server, select the **Install Kaspersky Security Center 13 Web Console** checkbox. Deselect the checkbox, if you want to install Kaspersky Security Center 13 Web Console later on the same device or separately on

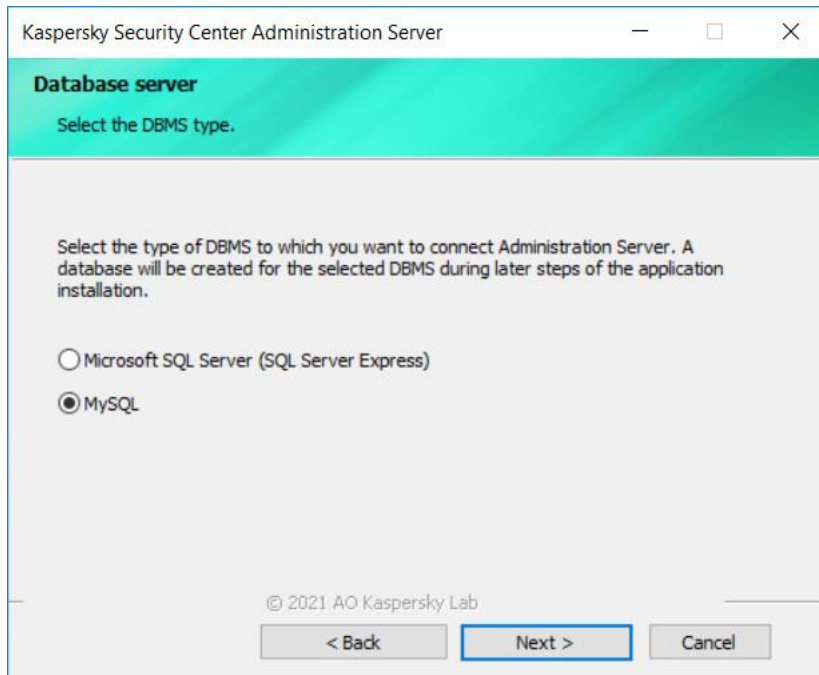
another device (the latter is of the evaluated configuration). Be aware that MMC-based console cannot be used in the evaluated configuration.



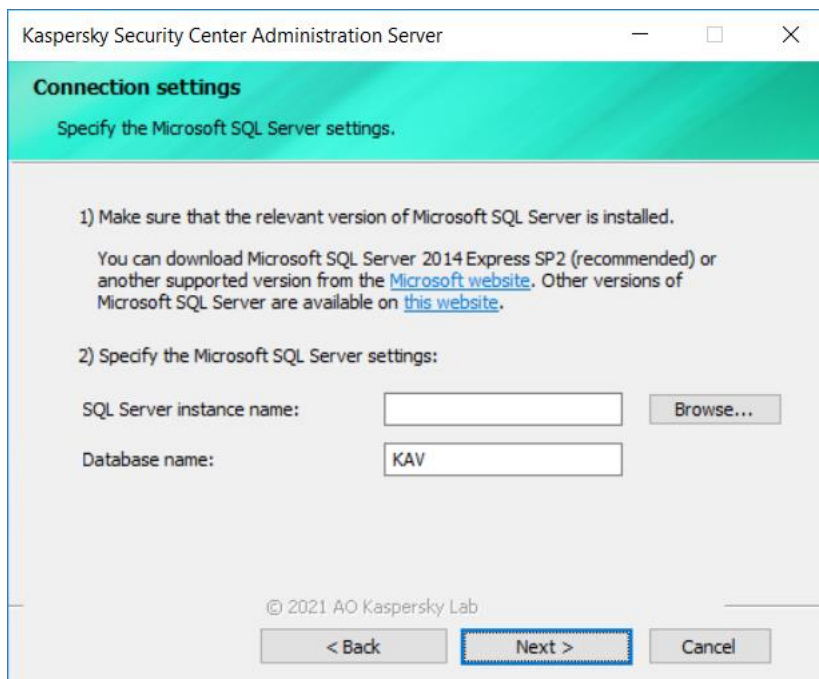
9. Select the size of your network. For the evaluated configuration keep the default **Fewer than 100 networked devices** value.



10. Select the type of database server that you installed earlier.



11. Specify the connection parameters for the database server that you have installed earlier.



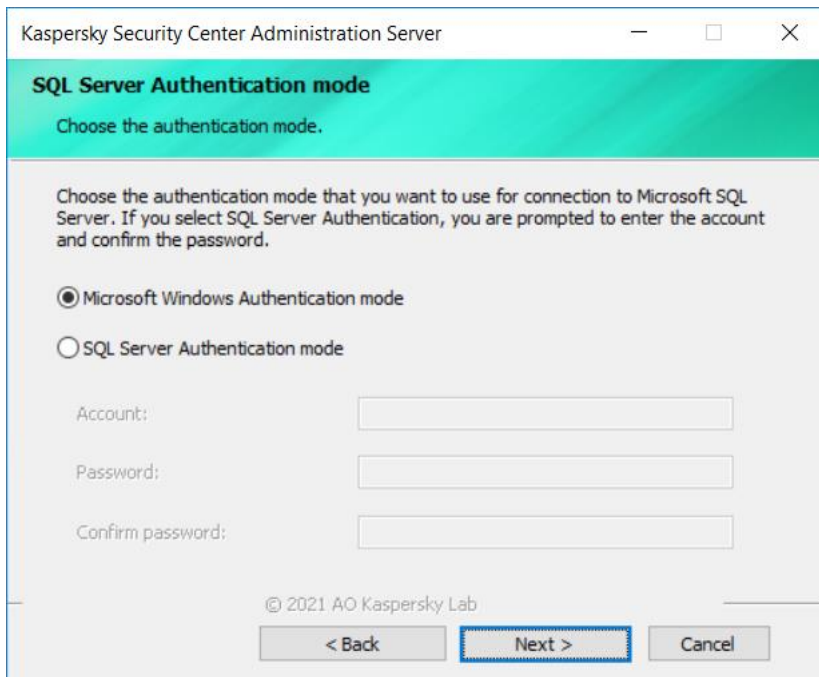
The image displays two sequential screenshots of the Kaspersky Security Center Administration Server configuration wizard.

First Screenshot: Connection settings
The window title is "Kaspersky Security Center Administration Server". The header is "Connection settings" with the instruction "Specify the MySQL Server settings." Below this, the user is prompted to "Select the device that has MySQL Server installed and specify the server port number and the database name." The form contains three input fields: "SQL Server instance name:" with the value "localhost", "Port:" with the value "3306", and "Database name:" with the value "KAV". At the bottom, there are three buttons: "< Back", "Next >" (highlighted with a blue border), and "Cancel". A copyright notice "© 2021 AO Kaspersky Lab" is visible above the buttons.

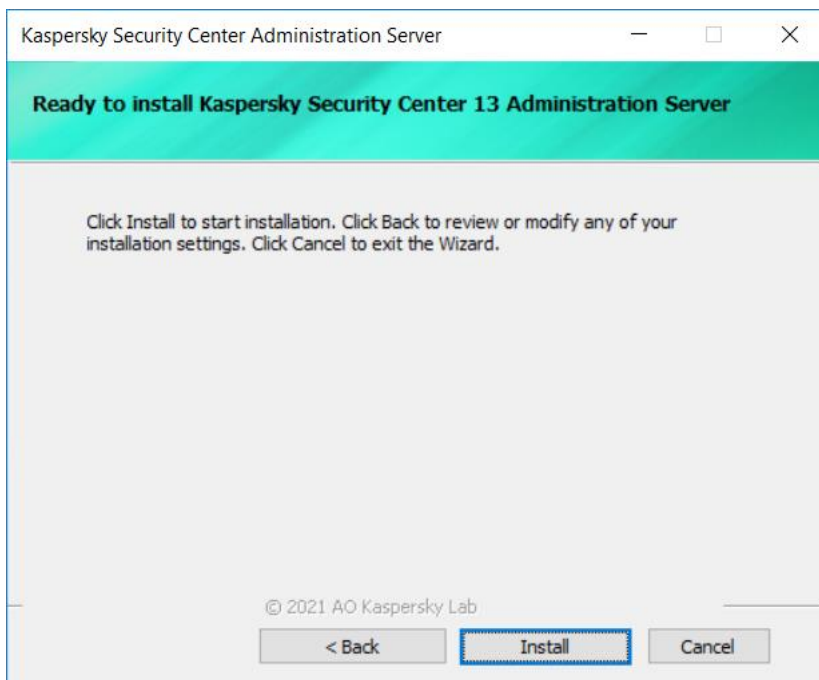
Second Screenshot: MySQL Server Authentication mode
The window title is "Kaspersky Security Center Administration Server". The header is "MySQL Server Authentication mode" with the instruction "Select MySQL Server Authentication." Below this, the user is prompted to "Select MySQL Server Authentication; you are prompted to enter the account and confirm the password." The form contains three input fields: "Account:" with the value "root", "Password:" with masked characters "••••••••", and "Confirm password:" with masked characters "••••••••". At the bottom, there are three buttons: "< Back", "Next >" (highlighted with a blue border), and "Cancel". A copyright notice "© 2021 AO Kaspersky Lab" is visible above the buttons.

12. Specify the authentication parameters for the database server that you have installed earlier.

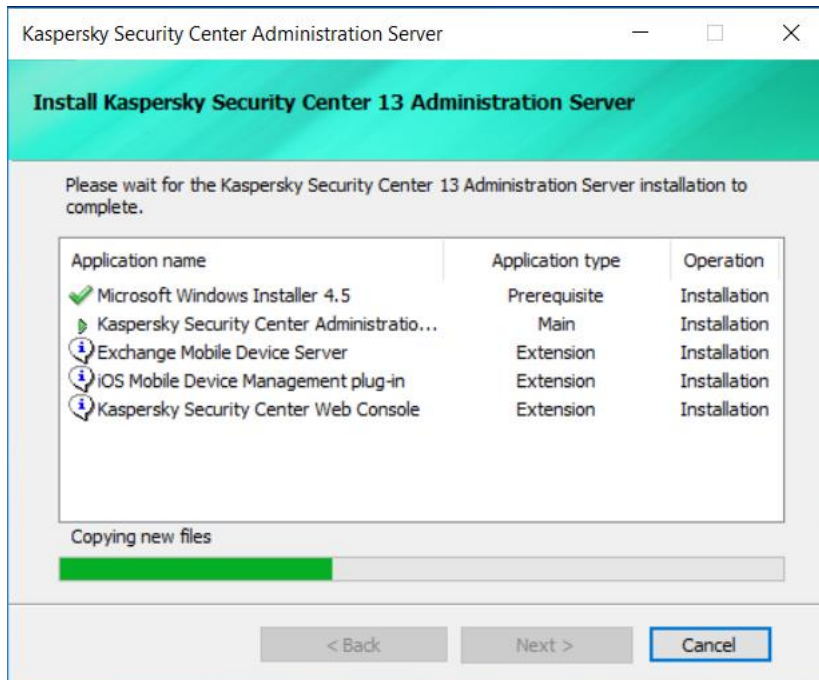
If the Administration Server account does not have access to the database server, which may occur when the database is stored on the device outside the domain or when the Administration Server is installed under a LocalSystem account, you should use SQL Server authentication mode.



13. Click **Install** to start the installation.



14. Please wait while the app is installing.



15. After the installation successfully completes, choose whether or not you want to start Administration Console right after you close the Wizard. You can open Kaspersky Security Center 13 Web Console only if it is already installed. You cannot open Kaspersky Security Center 13 Web Console if you did not install it during the installation of Kaspersky Security Center or if you have installed it separately on a different device.



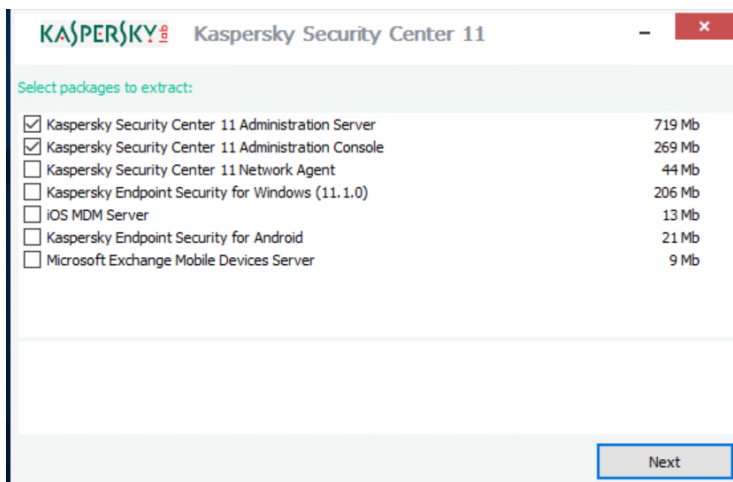
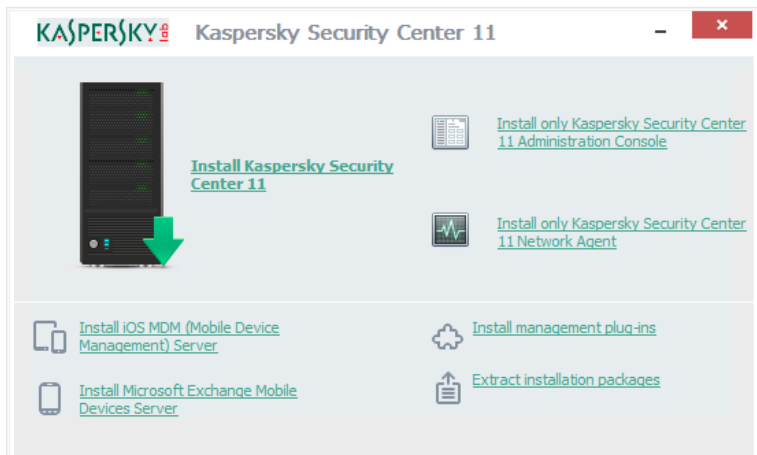
If you choose to open Kaspersky Security Center 13 Web Console, the login screen will open. Then you will be able to perform the initial configuration of the Administration Server by using the Quick Start Wizard (refer to the *Quick Start Wizard (Kaspersky Security Center 13 Web Console)* section of [UGD] for further instructions).

4.2. Web Console

Web Console uses a web-based user interface for interaction with KSC (Open API). Web Console has not been a part of evaluation of KSC, it is to facilitate the usage of web interface only.

4.2.1. Obtaining installation package

In order to obtain the Web Console installer, you may use **Extract installation packages** option of the KSC installer, select **Kaspersky Security Center 13 Administration Server** to extract.



Find the Web Console installer in Server\Packages\WebConsole\ directory of extracted package. The certified TOE package contains installer of Web Console version 13.0.10286. Please note that distribution page (see section 3.3) may contain a newer version of Web Console. It is recommended to use the latest available version of Web Console for better security.

4.2.2. Web Console Setup installation

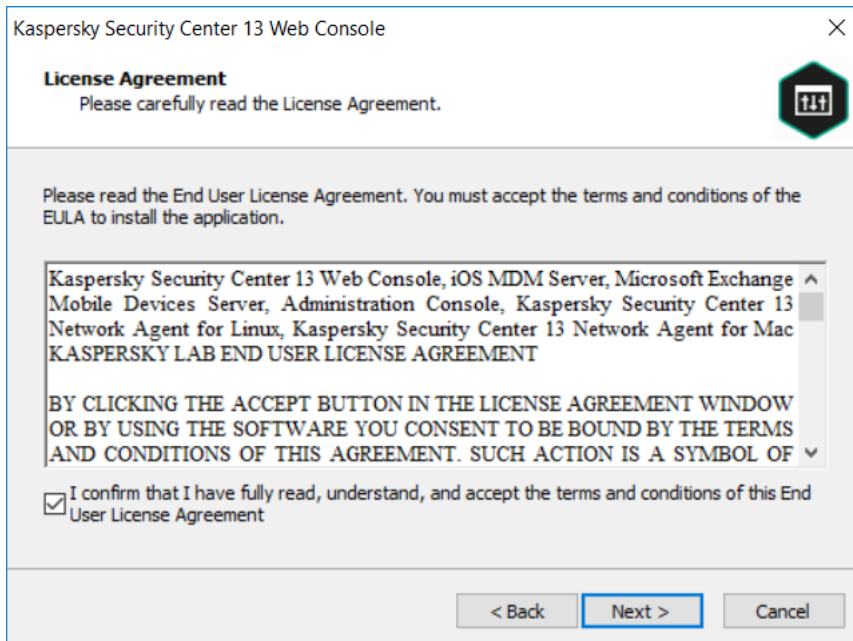
This procedure describes how to install Kaspersky Security Center 13 Web Console.

1. Make sure Node.js 14.16.1 is installed and system environment variable NODEJS_PATH is added to the OS.
2. Under an account with administrative privileges, run the `KSCWebConsoleInstaller.13.0.10286.exe` executable file. Note that numbers in *bold italic* may be different for other versions of Web Console.

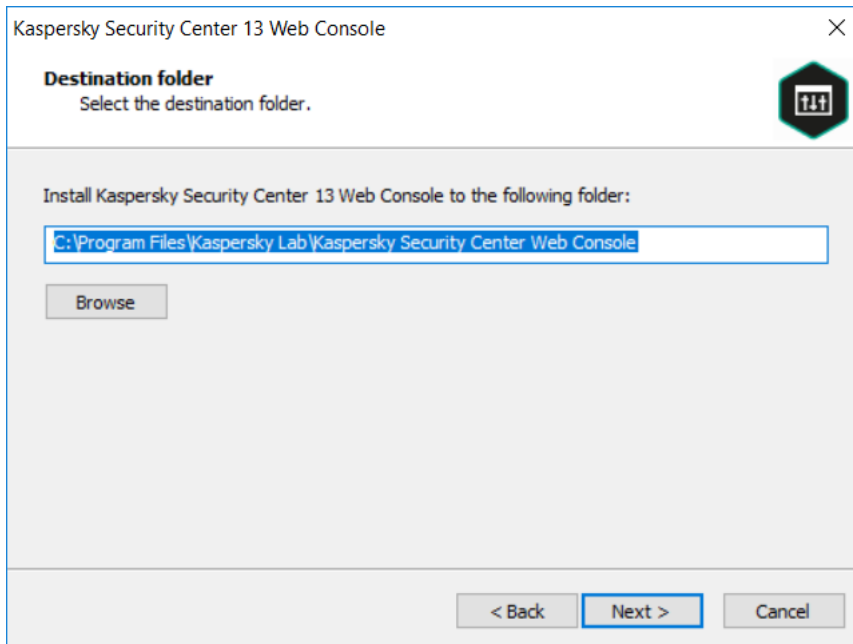
3. Allow the app to make changes to your device, if asked.
4. Select a language.
5. Setup Wizard starts. Click **Next**.



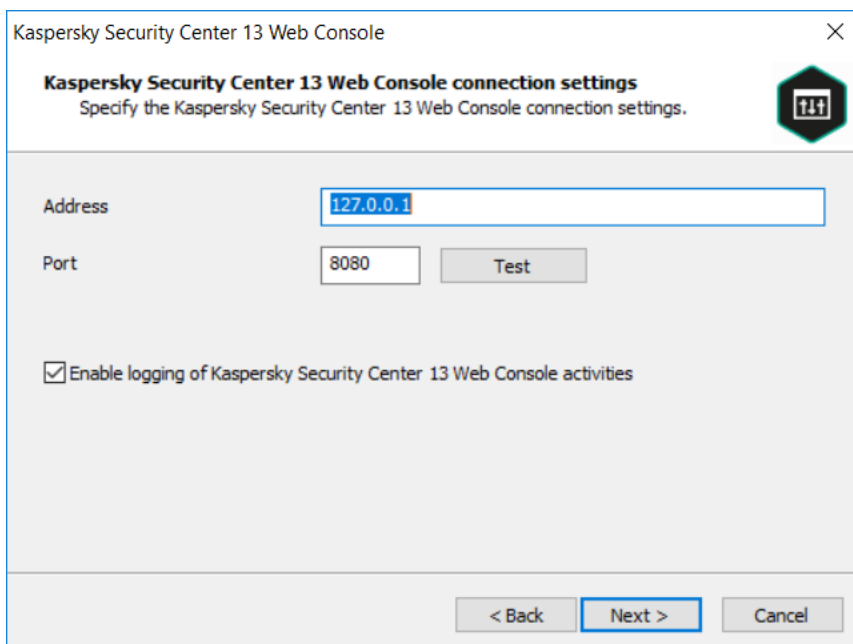
6. Read and accept the terms and conditions of License Agreement.



7. Specify a destination folder.



8. Specify the connection settings. This is the IP address and port to connect to Web Console via browser. By default, it is 127.0.0.1:8080.



- 9. Specify Node.js account settings if needed. You can use default or custom accounts.

Kaspersky Security Center 13 Web Console

Account settings
Specify the Kaspersky Security Center 13 Web Console account settings.

A Node.js account and update service account are required for starting and updating Kaspersky Security Center 13 Web Console. You can use the default accounts or specify custom ones.

Use default accounts
 Specify custom accounts

< Back Next > Cancel

Kaspersky Security Center 13 Web Console

Account settings
Specify the Kaspersky Security Center 13 Web Console account settings.

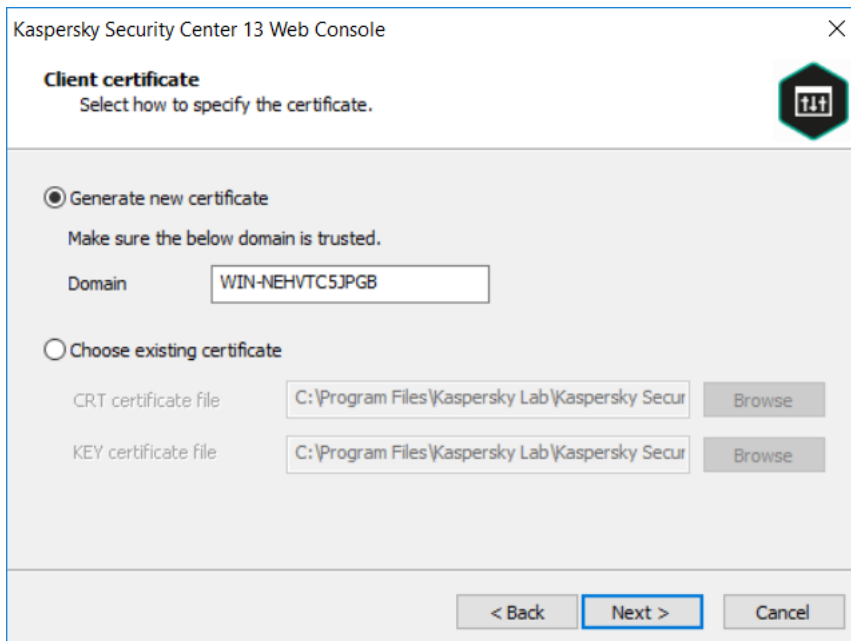
A Node.js account and update service account are required. The local user account must use a login in the ".\Administrator" format (account with administrator rights).

Node.js account
Login:
Password:

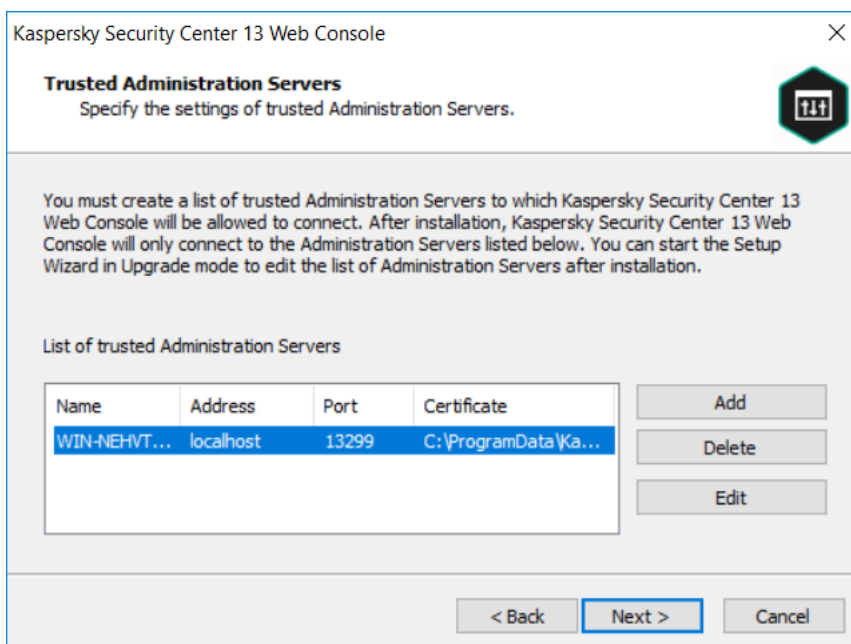
Update service account
Login:
Password:

< Back Next > Cancel

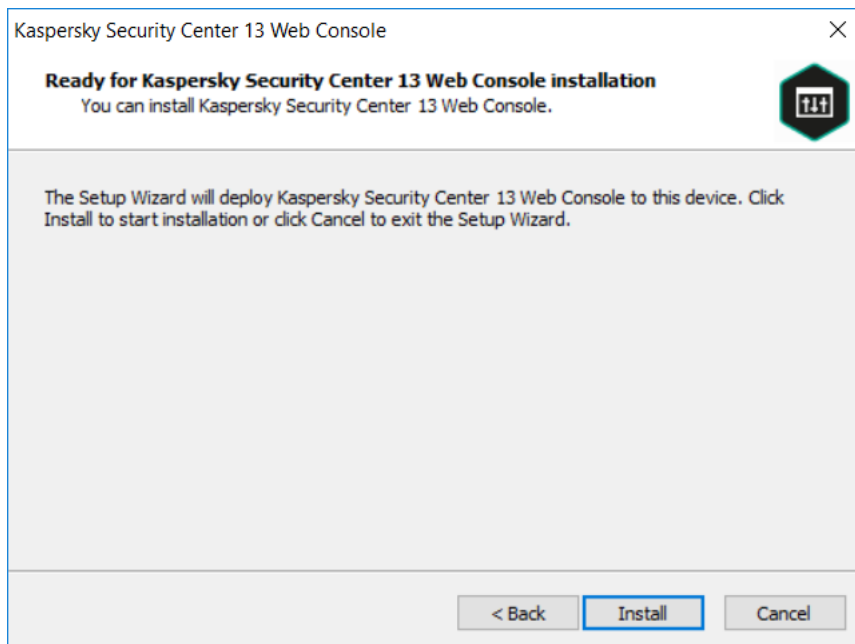
10. Select the way to specify the certificate of trust. You can either generate a new one or choose an existing one.



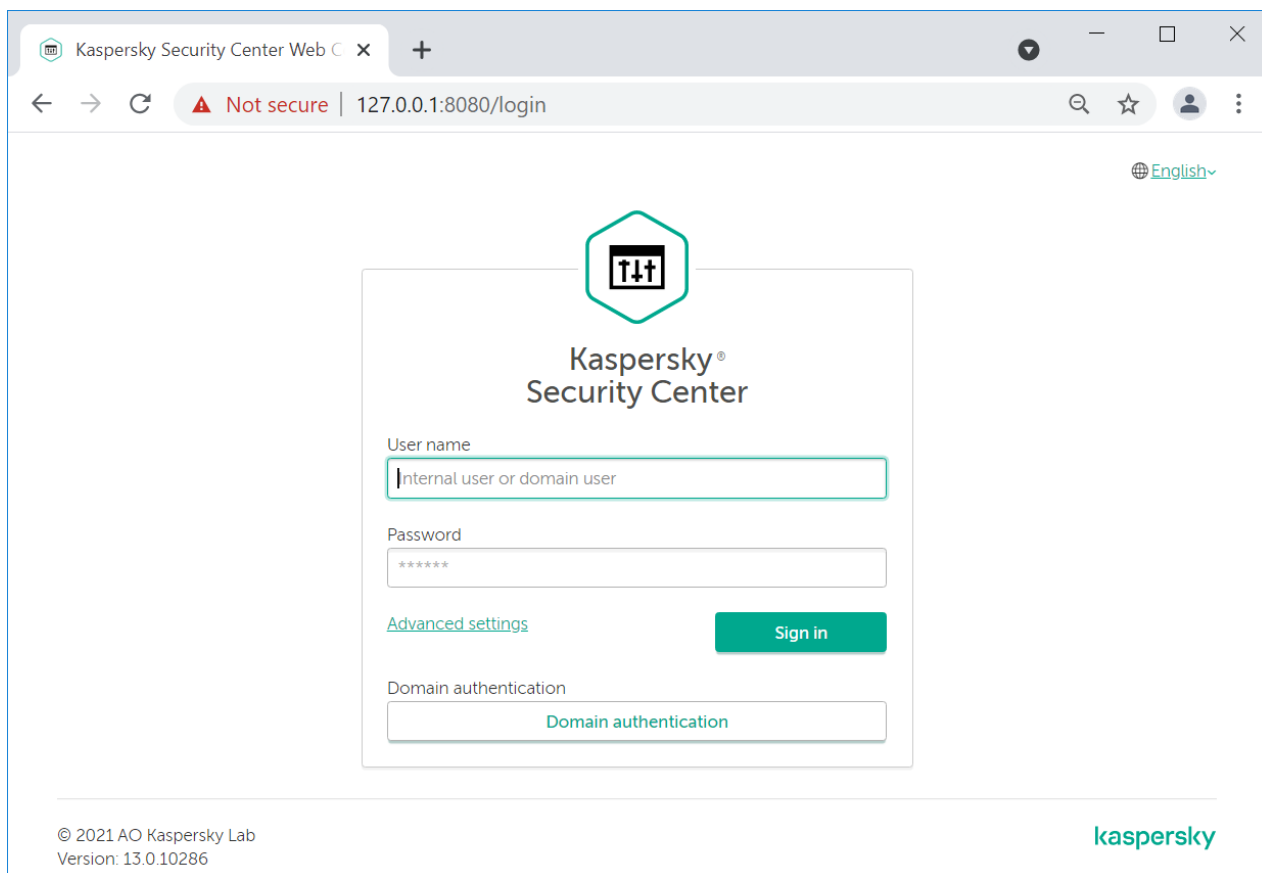
11. If you have chosen to generate a new certificate, you have to specify the settings of trusted Administration Server. Select one from the list or add a new one.



12. If Web Console is meant to be installed on the same device with Administration Server, IP address can have 'localhost' value. Otherwise specify the correct IP address and port. By default, Administration Server's certificate is located in C:\ProgramData\KasperskyLab\adminkit\1093\cert folder on the Administration Server device.

13. Click **Install**.

14. When installation is complete, you may use a web browser to open the Web Console user interface.



Be aware that the version shown at the bottom of login page relates to the version of Web Console, not KSC.

5. Post install setup

5.1. Quick Start Wizard

After installation is completed and Web Console is launched, the administrator should log in using credentials of a user with administrative privileges on a machine with Administration Server. Refer to “Logging in to Kaspersky Security Center 13 Web Console and logging out” section of [UGD], if needed.

After first logging in a tutorial window will appear.

Choose your tutorial scenario ✕

If you are new to Kaspersky Security Center, choose "New Administration Server". The main focus here is on the general functionality of Kaspersky Security Center and the Web Console features. Otherwise, if you are already familiar with the functionality, choose "Upgrade Administration Server". It will take you on a tour that demonstrates the difference between the on-premises and Cloud Console installation options, as well as migration and hybrid architecture.


[New Administration Server](#) [Upgrade Administration Server](#)

Select **New Administration Server** if you'd like to get acquainted with the interface. Tutorial mode will start. Go through it and after that Quick Start Wizard will launch.

Quick Start Wizard

Welcome | The Wizard setup may take as much as 15 minutes.

Welcome to the Quick Start Wizard of Administration Server WIN-NEHVTC5JPG8



This Wizard performs initial configuration of Administration Server and downloads updates. It also helps you to do the following:

- Activate Kaspersky Security Center 13
- Configure delivery of notifications by email
- Specify the proxy server settings

[Start](#)

It will allow for initial setup of important settings of KSC and create initial set of tasks and data for your installation. Refer to the [UGD] section “*Quick Start Wizard (Kaspersky Security Center 13 Web Console)*” for additional information, if needed.

Please note that you will be asked for activation key or activation code on one step of the wizard. It is safe to choose “Add license key later” option and continue setup.

5.2. Setting up roles

It is important to set up correct user access rights and policies immediately after the installation.

By default, OS administrator users also have KSC’s Main Administrator role privileges. You can setup separate users for this role, if needed. You may also want to add other users for less privileged roles. Refer to “*Users and user roles*” section of [UGD] for details.

5.3. Putting into evaluated configuration

5.3.1. Disabling mmc console ports (if MMC-based console is installed)

1. Open the system registry of the client device that has Administration Server installed (for example, locally, using the regedit command in the Start > Run menu).
2. Go to the following hive:
 - a. For a 64-bit system:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
 - b. For a 32-bit system:
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34\1093\1.0.0.0\ServerFlags
3. Create a DWORD key with the KLSRV_FLAG_PROHIBIT_GUI_PORT name.
4. Set the key value:1
5. Restart Administration Server service
 - a. net stop kladminserver
 - b. net start kladminserver

5.3.2. Setting minimum TLS version

1. Open the system registry of the client device that has Administration Server installed (for example, locally, using the regedit command in the Start > Run menu).
2. Go to the following hive:
 - a. For a 64-bit system:
HKEY_LOCAL_MACHINE\SOFTWARE\Wow6432Node\KasperskyLab\Components\34*.core\independent\
 - b. For a 32-bit system:
HKEY_LOCAL_MACHINE\SOFTWARE\KasperskyLab\Components\34*.core\independent\
3. Create hive Transport.
4. Create a DWORD key with the SrvUseStrictSslSettings name.
5. Set the key value:3

- Restart Administration Server service.

5.4. Setting the maximum number of events in the event repository

It is advised to set threshold and RBDMS size with regard to the number of managed endpoint devices, expected approximate number of received events and number of specialists who will be reviewing audit records.

To set limit of events refer to “Setting the maximum number of events in the event repository” section of [UGD].

5.5. Rolling out to endpoint devices

5.5.1. Manual installation

- Run the setup file of the endpoint machine.
- Choose “Install only Kaspersky Security Center 13 Network Agent”.



- This will initiate the installation wizard. You will be asked to accept EULA and choose installation folder.
- Manually fill in details for communication server consistent with your installation of KSC Administration Server.
- Provide proxy details, if needed.
- Choose “Do not use connection gateway”.
- Choose how encryption certificate will be obtained. For better security it is recommended to provide it manually.
- Define tags for managed machine (optionally), which may be used later for grouping managed endpoints in KSC interface.
- Specify advanced settings. Enable Network Agent service protection. Enable options for virtual compatibility, if needed.
- Choose if you want to start Network Agent application during installation or not.

11. Click **Install** to start the installation.
12. Complete installation wizard.

5.5.2. Centralised rollout

1. Login to Web Console.
2. Go to “Discovery & Deployment” > “Deployment & Assignment” > “Installation Packages”.
3. Select “Kaspersky Security Center 13 Network Agent (13.0.0.11247)” package.
4. Press “Deploy” button.
5. Select the deployment method for the selected installation package: Using the remote installation task.
6. Choose devices where you want to deploy Network Agent component. Refer to “Kaspersky Security Center 13 Web Console > Discovering networked devices” section of [UGD] to conduct initial discovery of devices via network polling.
7. You should choose means by which deployment will be conducted. Refer to “Kaspersky Security Center 13 Web Console > Protection Deployment Wizard” section of [UGD] for additional information regarding possible options on this and following steps. For initial installation you will have to use “Using operating system resources through Administration Server” option.
8. You choose restart process options on the next screen.
9. Select device assignment options.
10. You should provide wizard with the account with Administrator privileges for manage devices you are planning to deploy on.
11. Finish and run the task after the wizard.
12. Depending on the settings you made on Step 9 target machine will be listed in Discovery & deployment” -> “Unassigned devices” or “Devices” -> “Managed devices”
13. Refer to [UGD] for troubleshooting of those steps, if needed.
14. Clicking on the device name will open an Endpoint management window. Installed Network Agent and other managed AV products will be listed in Applications tab together with its versions.
15. For multiple Network Agent installations you should use Report on protection deployment from “Monitoring & Reporting > Reports” menu.

5.5.3. Rollout by external means

If you want to install Network Agent on a local device in non-interactive mode, execute the following command on the device:

```
msiexec /i "Kaspersky Network Agent.msi" /qn <setup_parameters>
```

where setup_parameters is a list of parameters and their respective values, separated by a space (PROP1=PROP1VAL PROP2=PROP2VAL).

The names and possible values for parameters that can be used when installing Network Agent in non-interactive mode are listed in the “Network Agent installation parameters” section of [UDG].

5.6. Checking KSC version installed

To check Administration Server and Network Agents versions installed do the following.

1. Open **Monitoring & Reporting** menu.
2. Go to **Reports** tab.
3. Select **Report on Kaspersky software versions** in Deployment section.
4. Report will show aggregated information about software versions.
5. Go to Details tab to view the list of devices and versions for each of KSC components ("Version number" column).
6. Make sure Kaspersky Security Center 13 Administration Server version and Kaspersky Security Center 13 Network Agents versions are all **13.0.0.11247**. This verifies that the correct versions of KSC components are installed, working and having successfully established connection between each other.



www.kaspersky.com/
www.securelist.com

© 2021 AO Kaspersky Lab.

All rights reserved. Registered trademarks and service marks are the property of their respective owners